



The Business Case for Desktop Authority Password Self-Service

A ScriptLogic Product Positioning Paper

The Business Case for Desktop Authority Password Self-Service

“I’ve forgotten my password!”

“I can’t log in!”

“Can you help me change my password? My old one just expired.”

“Why can’t I just re-use my old password? I can remember that one.”

Chances are that nearly one out of every three times the help desk or IT department picks up the phone, it’s for a password management issue. Passwords are necessary to provide the security and access management required by today’s enterprise. But are they costing you money?

On the one hand, password resets seem to demand an inordinate amount of IT attention. On the other hand, in an effort to ease the need to bother the help desk, end users often resort to non-secure password practices that may actually make the enterprise more vulnerable. Perhaps no other area of IT can offer the immediate return –on –investment (ROI), or end-user-enabling satisfaction than automation of password management. This white paper aims to detail the password management opportunity and the significant ROI organizations can achieve through the use of Desktop Authority Password Self-Service.

Why Passwords?

In modern enterprise networks, controlling the three “A’s”—*authentication, authorization, and access*—are all initiated by an end-user activity such as a login through a username and password. This practice may be avoided through other login methods—such as biometric and smart card logins—however, the vast majority of organizations still rely on the password login that ships with most operating systems.

Authentication is generally granted when the computer user verifies a user identity through something the user has (a username) and something the user knows (a password). Through this process, the operating system can verify the identity of the person logging in. Once the identity is verified—or authenticated—that identity is matched to the various rights granted to the employee by the organization. That is called authorization. The combination of authentication—verifying who you are; and authorization—establishing what you are able to see and do on the system—results in access, or the physical ability to see and do those things.

When the initiating authentication cannot occur—for example because a user can no longer remember his or her password, or the existing password has expired—authorization and thus access will not happen. The employee cannot do his or her job until authentication is reestablished and access is

once again granted. As a result, most organizations are stuck with passwords and the IT burden their management introduces.

The risk of giving uncontrolled access to valuable systems and data far outweighs the seeming benefit of eliminating passwords for convenience sake. With no login to identify the user, anyone could do anything they wanted on the network, which is a severe violation of virtually every IT regulation (such as Sarbanes-Oxley, HIPAA, and the Gramm-Leach-Bliley Act) and an unwise security practice.

The Challenge of Passwords

The fundamental dilemma organizations face is to strike the fine balance between security and efficiency. While it would be much more efficient to maintain a single password that is easy to remember and never changes for each user, the security implications make it unwise, and, in many cases, illegal. On the other hand, the most secure password would be one that is randomly generated, has no direct correlation to the demographics of the individual, and changes frequently. The problem with the more secure practice is that it would create passwords that are virtually impossible to remember, resulting in end users writing them down and/or involving the help desk for virtually every change.

Gartner reports:

“In attempts to improve password security or to appease auditors, enterprises may introduce or update policies that demand more-complex passwords and more-frequent password changes and which allow fewer failed login attempts. These policies tend to make users engage in riskier and more costly behavior regarding passwords. The harder passwords are to remember, the more likely it is that users will write them down and place the written list in an easy-to-find location or store passwords on a PC or handheld device without encrypting them. The majority of users who don’t write down or store hard-to-remember passwords are more likely to call the help desk for password resets.”¹

Many organizations are looking for tools to help enforce stronger password policies in an effort to increase security and enable regulatory compliance.

Another challenge is introduced when organizations use complex, multi-platform enterprises. While the majority of users would have a Windows login and password, any of those users that must access non-Windows resources—such as Unix/Linux systems, non-Windows applications, or mainframes and databases—must also have a login to those systems. Typically, the same rules for password length and complexity that are available in a Windows environment are not applicable on non-Windows systems. For example, the Windows password policy requires a password to be eight characters including at least two of the following: a capital letter, a special character or a number, and the password must be changed every 90 days. But many non-Windows systems, particularly older systems,

¹ *Toolkit: Evaluating Enterprise Options for Managing Passwords*, Gartner, 3 November 2006, ID Number G00144094

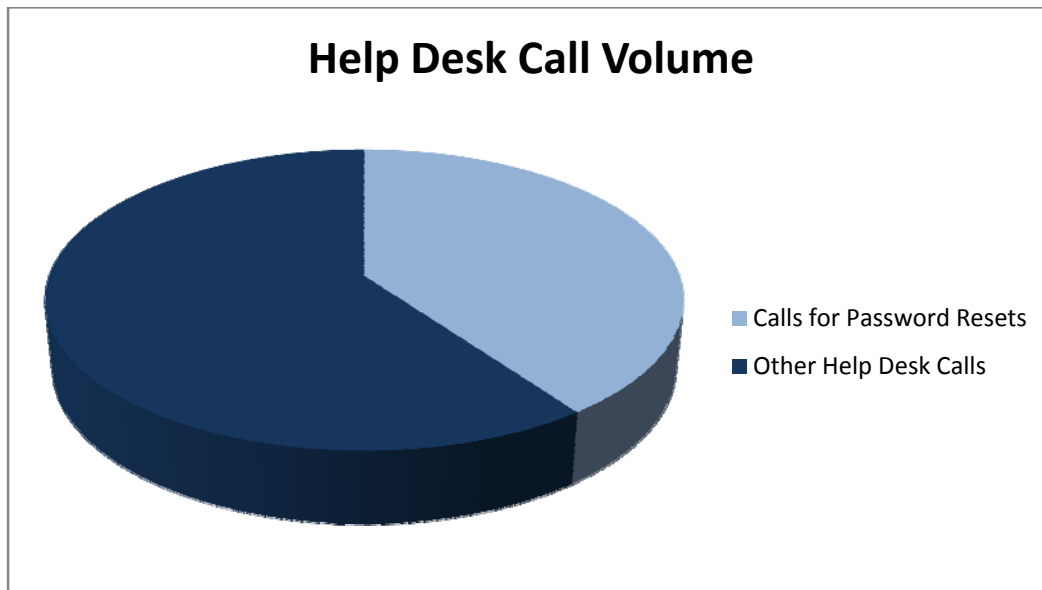
may not be able to handle passwords of such complexity. So the end user is left to create and remember a variety of passwords for a variety of systems and those passwords may be on different expiration cycles.

In many cases, an end user attempts to coordinate all systems with the same password. Unfortunately, the expirations rarely coincide, and resetting on one system requires resetting on all other systems as well. International Data Group (IDG) reports that an average user in a 10,000-employee organization has 14 separate passwords.

Exacerbating the problem further is the fact that different teams within IT often have responsibility for password management on different systems. For example, typically Windows password resets are handled by the Windows help desk, a relatively inexpensive resource. Password resets on Unix and Linux systems often must be handled by highly-paid and highly-skilled IT personnel with the knowledge and rights on those systems to maintain passwords. The more systems, the more passwords, and the more people that must be involved in a simple reset.

According Forrester

“Password problems and resets generally constitute between 25% and 40% of total help desk incidents.”²



Needless to say, even the most efficient organization probably admits password management as one of its most inefficient IT tasks. In reality, most organizations spend approximately 1/3 of their IT attention on password resets. In complex heterogeneous environments, these percentages can be much, much higher.

² *Twenty-Three Best Practices For The Customer Service Center*, Chip Gliedman, Forrester, October 11, 2005

The True Cost of Password Management

While it is difficult to place an exact cost on a single password reset call, analysts have been able to make some fairly accurate assumptions. Analysts place the cost of a typical password reset call at between \$10 and \$31. Add to this the lost productivity while end users deal with their password (rather than performing their job), which some analysts have placed at 20 minutes per incident, and the financial impact of manual password management practices can be significant.

One of the nation's largest banks estimated the monthly help desk expense for managing the 18 different passwords required for each user of their nationwide, heterogeneous enterprise at more than one million dollars a month. In a 2004 Gartner case study, a large beverage company determined that 30 percent of help desk calls were password-related with an average cost of \$17.23 per call for an annual impact of more than \$900,000³. Another organization—a large US-based utility—estimated a significant portion of its Tier 3, Unix IT staff's time was spent on Unix password management rather than on their core responsibilities.

Even if we assume the lowest numbers (\$10 per call and 15 percent of calls), it quickly becomes apparent that manual password management is one area that can deliver significant ROI through automation.

Automating Password Management

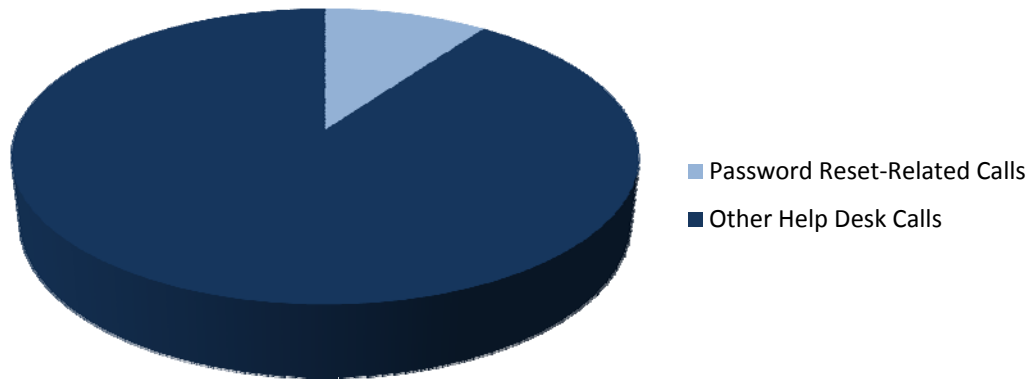
A number of products exist that can address the password management needs of organizations of all sizes. At the high end, we have comprehensive security frameworks—often called meta-directories—that include password management as one component of a comprehensive identity management offering. Not quite as expensive are products designed solely for password management on heterogeneous systems. Least expensive are password management solutions designed for a single platform—typically Windows—that may include integration with a meta-directory or directory consolidation product to deliver cross-platform coverage. For the sake of this paper, we will focus on the Windows/Active Directory (AD)-based password management with end-user self-service capabilities provided by Desktop Authority Password Self-Service.

Gartner estimates about 70 – 90 percent cost savings for help desks through the implementation of a self-service password reset solution⁴

³ *Automated Password Resets Can Cut IT Service Desk Costs*, Gartner, 13 December 2004, ID Number G00123531

⁴ *Toolkit: Evaluating Enterprise Options for Managing Passwords*, Gartner, 3 November 2006, ID Number G00144094

Help Desk Call Volume Savings with Desktop Authority Password Self-Service



At its very essence, Desktop Authority Password Self-Service provides the end-user community within an organization with the ability to change and reset passwords without involving the help desk or IT staff. It presents a series of challenge/response questions that end users must answer in order to unlock a locked account, change a password, or re-access systems once their failed logins have exceeded the limit.

In most cases, when a user cannot access his or her system due to a password issue, the user cannot access the self-service password reset application. Rather than require users to simply borrow a neighbor's PC to access the application, answer the questions, and reset the password or utilize kiosks whose sole purpose is password resets, Desktop Authority Password Self-Service allows web-based access to the application prior to login through a GINA extension on the desktop. Simply by clicking a "I forgot my password" link, the user is taken to a web page with password reset functionality is available.

Another major consideration is the elimination of multiple passwords entirely. Many organizations—such as our major banking and utility companies mentioned above—are undertaking sweeping initiatives to migrate Unix and Linux directories into AD. A natural byproduct of these efforts is the consolidation of multiple user identities (and thus multiple password requirements) into a single AD-based infrastructure. In these scenarios, an AD-based password management tool—including self service—can serve the needs of the entire cross-platform enterprise. The large bank discussed earlier, saw an immediate reduction of 35 percent in help desk calls as a direct result of consolidating user identities and passwords from 18 to 2. Similarly, the utility company estimates annual savings of nearly a million dollars simply by moving many tasks—such as password resets—from expensive Unix IT personnel to the Windows help desk. Therefore, while Desktop Authority Password Self-Service focuses solely on AD-based passwords, it is evident that consolidating directories in conjunction with a password management solution can have a positive impact on manageability.

Calculating Return on Investment

Based on a conservative use of the numbers provided by analyst firms, the following ROI can be experienced through implementing Desktop Authority Password Self-Service to manage AD-based passwords. We use a 1,000-user company as an example and a cost of \$5.60/seat for the Desktop Authority Password Self-Service.

Employee Data	
Number of Users	1,000
Average fully-burdened salary of user (employee)	\$50,000
Annual fully-burdened salary of help desk associate	\$50,000
Hours in a single work year	2,080 hours

Help Desk Metrics	
Help desk calls per user each year	10
Percentage calls related to password reset	40%
Average duration password reset call	15 mins./call
Average user inactivity for password issue	20 mins./call

Without a Password Management Solution	
Total number of help desk calls per year	10,000
Total help desk calls for password incidents	4,000
Total annual help desk time spent on password reset calls	1,000 hours
Total annual user inactivity wasted on password reset calls	1,333 hours
Cost of user's time lost for each incident	\$8.01 per call
Cost of help desk for each incident	\$6.01 per call
Total cost of user inactivity without password management solution	\$32,051
Cost of password reset help desk calls	\$24,038
Total Cost without Password Management Solution	\$56,089

With a Password Management Solution	
Percentage of password calls handled by solution	100%
Total number of calls covered	4,000
Average duration self-serve password reset session	3 minutes
Total cost of user inactivity for users with solution	\$4,807
Cost of password reset help desk calls	\$0
Total Cost with Password Management Solution	\$4,807

ROI Analysis	
Annual savings with Desktop Authority Password Self-Service	\$51,282
Less Upfront Software Investment	(\$5,600)
One Year Dollar Savings	\$45,682
Benefit as a Multiple of Cost	8.1x
Payback Period on Investment	1.3 Months

Conclusion

Obviously, the ROI for implementing a self-service password reset solution is significant. This benefit can be even further enhanced when the solution is combined with technologies that reduce the overall number of passwords that must be managed. No other identity management practice can bring the financial benefit, security enhancements, and compliance enabling practices that come with an automated password management solution. Simply enabling end-user self service can dramatically reduce costs and increase efficiency. In addition, using Desktop Authority Password Self-Service can provide significant improvements in security and compliance. And those benefits are multiplied as the same technologies apply to heterogeneous systems beyond Windows and AD.